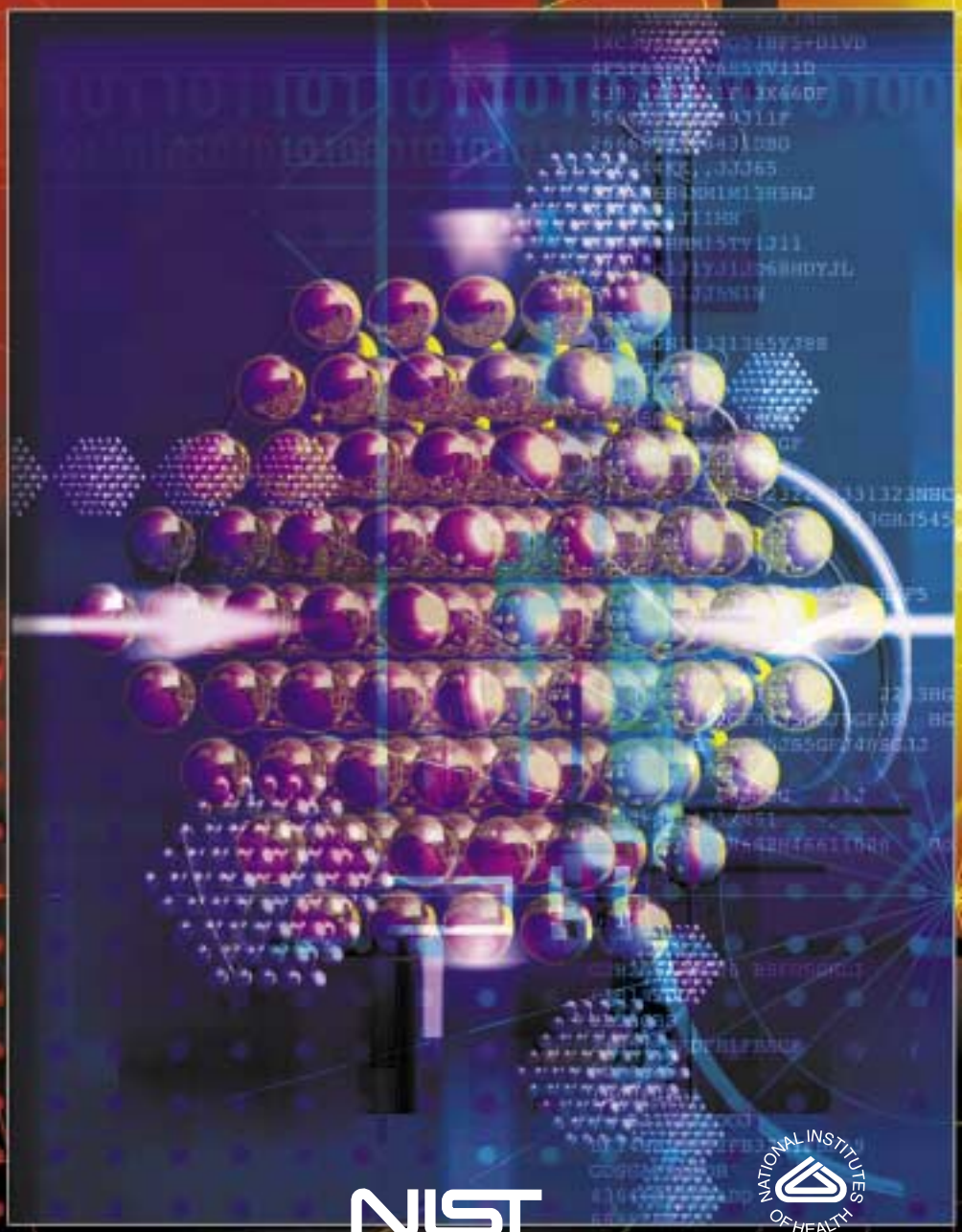
2nd Annual PKI Research Workshop



April 28-29, 2003

NIST

Gaithersburg, MD

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

National Institutes of Health

Internet2

2nd Annual PKI Research Workshop

NIST ■ Gaithersburg, MD ■ April 28–29, 2003

Sponsored by
National Institute of Standards and Technology
National Institutes of Health
and Internet2
in cooperation with USENIX, the PKI Forum and IFIP TC8

Most PKI implementations today are used to bind identities to public keys and manage the revocation of the resulting certificates. This workshop, however, considers the full range of public key technology used for security decisions. At the "relying party" end, where the certificates are actually used, completing a transaction includes discovery and interpretation of relevant security information the validity of which is verified against appropriate roots of authority. There are many security decisions (concerning authentication and authorization) to be made and they need to be made correctly. All of this needs to occur with tools that are simple to use correctly (by developers and by end-users) and pleasant enough that one would choose to use them.

This workshop among leading security researchers will explore the issues relevant to this area of security management, and will seek to foster a long-term research agenda for authentication and authorization in populations large and small via public key cryptography. The workshop is intended to promote a vigorous and structured discussion among the leading academic and corporate developers and the user community—a discussion well-informed by the problems and issues in deployment today.

We solicit papers, panel proposals, and participation.

Submitted works for panels and papers should address one or more critical areas of inquiry. Topics include (but not are not limited to):

- Cryptographic methods in support of security decisions
- The characterization and encoding of security decision data (e.g., name spaces, x509, SDSI/SPKI, PGP, XKMS, SAML, WSS), policy mappings and languages, etc.
- The relative security of alternative methods for supporting security decisions. Risk management.
- Correctly interpreting the results of a private key operation or a public key operation. Interpreting signed objects that have active code.
- Key management and rollover, and certificate management and rollover
- Privacy protection and implications of different approaches
- Scalability of security systems—are there limits to growth?
- Security of the various components of a system: private keys, root authorities, certificate storage, communications channels, code, directories, etc.
- User interface issues with naming, multiple private keys, selective disclosure
- Mobility solutions
- Approaches to attributes and delegation
- Discussion of how the "public key infrastructure" may differ from the "PKI" traditionally defined
- User Interface issues in PKI tool construction, and the security implications of different UI choices
- Reports of real-world experience with the use and deployment of PKI, especially where future research directions for PKI are indicated
- What is missing? The gaps in PKI reasarch and standards from a systems engineering point-of-view

Deadlines for conference paper and panel submission are:

- **Papers and Proposals Due: January 31, 2003**
- **Authors Notified: March 7, 2003**
- **Final Materials Due: April 4, 2003**

Full instructions will appear on the workshop web site,
http://middleware.internet2.edu/pki03/

PROGRAM COMMITTEE

Peter Alterman, *NIH*
Matt Blaze, *AT&T Labs Research*
Bill Burr, *NIST*
Yassir Elley, *Sun Microsystems*
Carl Ellison *(chair), Intel*
Stephen Farrell, *Baltimore Technologies*
Richard Guida, *Johnson and Johnson*
Peter Honeyman, *University of Michigan*
Ken Klingenstein, *University of Colorado*
Neal McBurnett, *Internet2*
Clifford Neuman, *USC*
Eric Norman, *University of Wisconsin*
Tim Polk, *NIST*
Ravi Sandhu, *George Mason University*
Krishna Sankar, *Cisco Systems*
Frank Siebenlist, *Argonne National Laboratory*
Sean Smith, *Dartmouth College*
Michael Wiener, *Independent*

REGISTRATION

The registration fee of **$105** per person includes workshop materials, coffee breaks, lunches, and a dinner. Please complete and return the attached interest card by, **February 11, 2002.** Further agenda and registration information will be forwarded in February to all who respond.

Electronic registration is available at: www.nist.gov/conferences.

ACCOMMODATIONS

A block of rooms has been reserved at the Gaithersburg Holiday Inn, **(301) 948-8900** at a special rate of **$90** single or double, plus 12% tax. Reservations must be received by **April 10, 2003.**

TECHNICAL INFORMATION

General Chair:
Ken Klingenstein, *University of Colorado*
Ken.Klingenstein@Colorado.edu

Program Chair:
Carl Ellison, *Intel Corporation*
cme@jf.intel.com

Steering Committee Chair:
Neal McBurnett, *Internet2*
neal@bcn.boulder.co.us

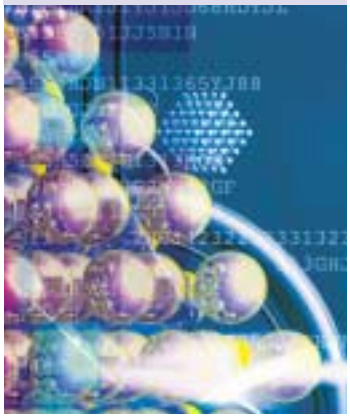
Local Arrangements Chair:
Nelson Hastings, *NIST*
nelson.hastings@nist.gov

REGISTRATION INFORMATION

Kim Snouffer
NIST
Phone: (301) 975-2776
Fax: (301) 948-2067
email: kimberly.snouffer@nist.gov

VISIT THE CONFERENCE WEB SITE

http://middleware.internet2.edu/pki03/



2nd Annual PKI Research Workshop

NIST ■ Gaithersburg, MD
April 28–29, 2003

Please place in an envelope and return by **FEBRUARY 10, 2003** to:
Kim Snouffer
NIST
100 Bureau Dr., Stop 3461
Gaithersburg, MD 20899-3461
or fax to:
Kim Snouffer, (301) 948-2067

NAME _____

TITLE _____

ORGANIZATION _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

PHONE _____ FAX _____ E-MAIL _____